UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753

7590 05/24/2004

Docket Administrator Rm 3C 512
Lucent Technologies Inc
600 Mountain Avenue
P O Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	5

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/578,633	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 14-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,4-12,14-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Office Action

Claims 4 and 13 have been canceled. Claims 1-3, 4-12, 14-27 have been fully reconsidered and are pending.

Response to Amendment

The amendment to claims 1-3, 4-12, 14-27, specifically the added limitation, "the security characteristic being a measure of connectivity between the first communications network and the second communications network" renders the claims indefinite and are not rejected under 35 USC 112 2nd paragraph which states:

> The following is a quotation of the second paragraph of 35 U.S.C. 112:
>
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Examiner finds the claims, which this limitation indefinite because it is unclear as to what Applicant regards as the security characteristic. The language of the claims, claim 1 in particular, states the security characteristic is determined as a function of a response by the probed host but there is not a clear indication as to whether the security characteristic is an entity or quantity. The security characteristic could be interpreted as a packet, a probe echo, a firewall, or even some indication of connection. The claim language, which states the security characteristic is a measure of connectivity, further adds to the ambiguity of the claim. The American Heritage College Dictionary defines measure as:

1. Dimensions, quantity, or capacity as ascertained by comparison with a standard.
2. A reference standard or sample used for the quantitative comparison of properties: *The standard kilogram is maintained as a measure of mass.*
3. A unit specified by a scale, such as an inch, or by variable conditions, such as a day's march.
4. A system of measurement, such as the metric system.
5. A device used for measuring.
6. The act of measuring.
7. An evaluation or a basis of comparison: "the final measure of the worth of a society" (Joseph Wood Krutch).
8. Extent or degree: *The problem was in large measure caused by his carelessness.*
9. A definite quantity that has been measured out: *a measure of wine.*
10. A fitting amount: *a measure of recognition.*
11. A limited amount or degree: *a measure of good-will.*
12. Limit; bounds: *generosity knowing no measure.*
13. Appropriate restraint; moderation: "The union of... fervor with measure, passion with correctness, this surely is the ideal" (William James).
14. An action taken as a means to an end; an expedient. Often used in the plural: *desperate measures.*
15. A legislative bill or enactment.
16. Poetic meter.
17. *Music.* The metric unit between two bars on the staff; a bar.

Definition 1 states that measure is a quantity whereas definition 5 defines a measure as a device. Therefore the security characteristic could be either a quantity or a device. Because the two meanings are so different, Examiner is unclear as to which the Applicant regards as his invention. For purposes of this office action, Examiner is

interpreting the claim to mean an indication of connectivity between the first and second communications networks. Examiner equates this indication of connectivity to the teaching in Shostack et al where the network is scanned to reveal all of the network connections to generate a map of the network (column 12, lines 47-55).

Response to Arguments

Applicant has argued on pages 9-10 that there is a distinction between the spoofing taught by the Applicant and the prior art Shostack et al. Examiner would like to address this argument in several ways. Examiner understands that in the Applicant's specification, spoofing is used to discover possible security risks. As indicated by Applicant, Shostack et al teach that spoofing is a potential means to compromise a system. Examiner does not find the prior art to teach how to spoof in a malicious way. The prior art mentions attacks which pose threats to computer network. Examiner understands the prior art to teach and suggest that a network administrator or the automated security management system to simulate known attacks, not for the malicious purposes, but to make sure the system would not fall be jeopardized by a malicious spoof attack (column 3, lines 1-5).

Examiner assumes the Applicant is making distinction between using a spoof probe packet to find connections in a network and using a spoof probe packet to determine is the network will block those packets from ever getting into the network. However, the Examiner finds in the Shostack et al reference that the simulated attacks

are conducted from a second network (column 13, lines 1-10). If a spoof probe packet is directed at a network from the outside and is somehow returned, that would mean there is a positive connectivity between an outside host and a host on the inside of the "secure" network. For the record, Examiner finds the Shostack et al reference to suggest and teach using spoofed packets from outside the network as a means to discover potentially unsecure hosts in a network.

If Applicant is not convinced that the Shostack et al reference does not teach using a spoof probe packet, Examiner would also like to point out that the claimed invention does not claim a spoofed probe packet. Applicant does define a spoofed probe packet in the specification on page 9, line 23-30. However, only a probe packet is claimed and the Applicant indicates on page 11, line 4 that a spoof probe packet is an example of a probe packet. This means that the probe packet of the claimed invention does not necessarily have to relate to a spoof probe packet.

In view of this foregoing remarks the Examiner respectfully disagrees with Applicant and maintains that the claimed invention as amended is not patentably distinct from the prior art of record.

Claim Rejections - 35 USC § 112

Claims 1-3, 4-12, 14-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention for the reasons mentioned in the immediate office action.

Claim Rejections - 35 USC ' 102

Claims 1-3, 5-12, and 15-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al (USP 6,298,445).

As per claims 1 and 24, Shostack et al teach a communications network security method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address determined as a function of the topology (column 12, lines 41-57); and

determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claims 2 and 25, Shostack et al teach the source address is an IP address associated with a host external to the communications network (column 1, lines 64-65 and column 3, lines 1-4).

As per claims 3 and 26, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 5, Shostack et al teach the probing the at least one host operation further comprises:

the first and second communications network have different security levels, and the measure of connectivity is a function of whether the probed hose of the first communications network communications with the external host associated with the second communications network (column 13, lines 1-10).

As per claim 6, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 7, Shostack et al teach the first and second communications network have different security levels (column 13, lines 1-5).

As per claim 8, Shostack et al teach the transmitted packet is a TCP packet (column 5, lines 24-45).

As per claim 9, Shostack et al teach the second packet is a UDP packet or an ICMP packet (column 5, lines 24-45).

As per claim 10, Shostack et al teach a method for analyzing network security of a communications network, the method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts internal to the communications network as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

transmitting a packet from a host external to the communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet being generated as a function of an IP address associated with the host external to the communications network and an IP address associated with the particular one host of the plurality of hosts internal to the communications network (column 13, lines 1-6); and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claim 11, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19), the security characteristic being a measure of connectivity between the first

communications network and the second communications network (column 13, lines 1-5).

As per claim 12, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 15, Shostack et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (column 9, lines 10-18).

As per clam 16, Shostack et al teach a communications system comprising:

a first plurality of computers associated with a first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the plurality of computers, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5) performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP address associated with a

second computer of the second plurality of computers and an IP address associated with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet (column 12, lines 41-57, column 1, lines 64-65, and column 3, lines 1-4).

As per claim 17, Shostack et al teach the security host computer is associated with the first communications network (column 4, lines 33-34).

As per claim 18, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 19, Shostack et al teach the determining the security characteristic operation further comprises:

> monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claims 20 and 27, Shostack et al teach the first communications network is an intranet and the second communications network is an Internet (column 4, lines

14-21) and the two network communications have different security levels (column 13, lines 1-5).

As per claim 21, Shostack et al teach a security host computer comprising:

means for performing a census of a communications network and determining a topology of a first communications network, the topology being defined by at least one computer (column 12, lines 41-57);

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of the topology, an IP address associated with a particular host computer associated with a second communications network and an IP address associated with the computer, the second communications network being separate from the first communications network (column 12, lines 41-57); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet (column 12, lines 41-57) the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5).

As per claim 22, Shostack et al teach the determining the security characteristic operation further comprises:

> monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 23, Shostack et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (column 4, lines 14-21).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100